UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/500,792	03/21/2005	Sebastien Canard	5284-40PUS	8286

27799 7590 12/16/2008

COHEN, PONTANI, LIEBERMAN & PAVANE LLP
551 FIFTH AVENUE
SUITE 1210
NEW YORK, NY 10176

EXAMINER	
PHAM, LUU T	

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
12/16/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/500,792	CANARD ET AL.	
	Examiner	Art Unit	
	LUU PHAM	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 October 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,10 and 11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,10 and 11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to the Amendment filed on 10/17/2008.

2. In the instant Amendment, Claims 6-9 were cancelled; Claims 1-5 and 10-11 have been amended; Claims 1, 10, and 11 are independent claims. Claims 1-5 and 10-11 have been examined and are pending. **This Action is made FINAL**.

Response to Arguments

3. The objection to the specification is withdrawn as the specification has been amended.

4. The rejections of claims 6 and 10 under 35 U.S.C. § 101 are withdrawn as the claim 6 was cancelled and claim 10 has been amended.

5. The rejections of claims 1-11 under 35 U.S.C. § 112, second paragraph, are withdrawn as the claims 6-9 were cancelled and claim 1-5 and 10-11 have been amended.

6. Applicants' arguments with respect to claims 1-5 and 10-11 have been fully considered but they are not persuasive.

Applicants' arguments:

a. *"Camenisch thus fails to teach or suggest 'an additional signature of a combination comprising the message and the anonymous signature using the up-to-date common private key of the signing member,' as now recited in amended independent claim 1."*

b. *"The skilled person would have no reason to combine the teachings of Camenisch with the teachings of Inada to achieve the subject matter of independent claims 1, 10 and 11, absent impermissible hindsight;" and "the skilled person would have*

no reason to combine the teachings of Camenisch and Inada with the deletion protocol of Kim in the Examiner's proffered manner, absent impermissible hindsight based on applicants' instant disclosure."

The Examiner disagrees for the following reasons:

a. Camenisch does teach an additional signature of a combination comprising the message and the anonymous signature using the up-to-date common private key of the signing member *(Camenisch: pages 102-103 and 107-108; sections 5.4.3, 5.4.4, 5.5.3, and 5.5.4; signing messages and opening signature;*

$V_1 := SPK_{14}\{(\beta): d\widetilde{g} = \widetilde{g}^{\beta'}\}(m)$ and

$V_2 := SPK_{12}\{(\alpha): d = \widetilde{g}^{\alpha''}\}(V_1)$;

also

$V_1 := SPK_7\{(\gamma,\delta): \widetilde{z} = \widetilde{g}^{\gamma} \wedge d_2 = h^{\delta} \wedge d_1 = y_R^{\delta} g\gamma\}(m)$;

$V_2 := SPK_{14}\{(\beta): \widetilde{z}\widetilde{g} = \widetilde{g}^{\beta'}\}(V_1)$;

$V_3 := SPK_{12}\{(\alpha): d = \widetilde{g}^{\alpha''}\}(V_2)$;

wherein V_2, and V_3 are known as additional signatures).

b. In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure,

such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971). In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Inada with the method and system of Camenisch to include steps of encrypting a common private key of said asymmetrical keys common to said members of the group using each of said symmetrical secret keys to obtain as many encrypted forms of said common private key as there are non-revoked members; and a smart card associated with each member in the group to allow an arbitrary member in a group to decrypt and write a signature by use of a group key which is allowed to be used by only the group member *(Inada: col. 1, lines 9-12)* and it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Kim with the method and system of Camenisch and Inada wherein means for updating said common private key stored in the storage means of the each member to update said common private key only if one encrypted value of said common private key calculated by

said first calculation means may be decrypted using said symmetrical secret key in said storage means of the each member to allow member deletion and sign-tracing generated by a specific member *(Kim: page 151, lines 15-16)*.

Claim Objections

7. **Claim 4 is objected to** because of the following informalities:

- There is a typo in line 2: *"further* ***omprising****:"* (emphasis added). Appropriate correction is required.

8. **Claim 5 is objected to** because of the following informalities:

- There is a typo in line 2: *"****wherein the further*** *further comprising:"* (emphasis added). Appropriate correction is required.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to

point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

11. **Claims 1 and 10-11 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Camenisch, "*Group Signature Schemes and Payment Systems Based on the Discrete Logarithm Problem,*" Doctor of Technical Science, Swiss Federal Institute of Technology Zurich, 1998, and in view of Inada, U.S. Patent No. 6,986,044, filed on August 31, 1999, and further in view of Kim et al. (hereinafter "Kim"), "Efficient and Secure Member Deletion in Group Signature Schemes," D. Won (Ed): ICISC 2000, LNCS 2015, pp. 150-160, Springer-Verlag Berlin Heidelberg, 2001.

- **Regarding claim 1**, Camenisch discloses a cryptographic method of anonymously signing a message by a member of a group comprising a plurality of members each equipped with calculation means and associated storage means *(page 71, lines 4-18)*, the method initially comprising:

a first step of calculating, at first calculation means of a trusted authority a pair of asymmetric keys common to the members of the group and comprising a common public key and a common private key *(Camenisch: page 100, section 5.4.1, lines 19-21; page 105, section 5.5.1, lines 16-17; RSA public key (n,e), the primes p and q are her secret key)*;

a second step of calculating, at the first calculation means of the trusted authority, a group public key associated with the members of the group *(Camenisch: page 101, lines 1-3; page 105, section 5.5.1, lines 29-30; group public key Y)*;

a third step of calculating, during an interaction between the calculation means of the trusted authority and the calculation means of the member, a group private key for each member of the group and storing the private key in the storage means of the each member, each group private key being associated with the group public key and being different for each member of the group *(Camenisch: pages 101-102, section 54.2; pages 106-107, section 5.5.2: Generating Membership Keys and Certificate; Arto joins the group, obtains membership certificate, stores x, y, and v securely)*;

a fourth step of determining, at the first calculation means of the trusted authority, as many symmetrical secret keys as there are members of the group *(Camenisch: page 74, lines 13-15; a secret key x_i to each group member P_i)*; and

when a non-revoked group member anonymously signs message to be sent to an addressee, the method further comprising:

a ninth step of calculating, at the calculation means of the signing member, an anonymous signature of the message using the group private key for the signing member *(Camenisch: pages 102-103 and 107-108; sections 5.4.3, 5.4.4, 5.5.3, and 5.5.4; signing messages and opening signature)*; and

a tenth step of calculating, at the calculation means of the signing member, an additional signature of a combination comprising the message and the anonymous signature using the up-to-date common private key of the signing member *(Camenisch:*

pages 102-103 and 107-108; sections 5.4.3, 5.4.4, 5.5.3, and 5.5.4; signing messages and opening signature; $V_1 := SPK_{14}\{(\beta) : d\tilde{g} = \tilde{g}^{\beta'}\}(m)$ and $V_2 := SPK_{12}\{(\alpha) : d = \tilde{g}^{\alpha'}\}(V_1)$; *also* $V_1 := SPK_7\{(\gamma, \delta) : \tilde{z} = \tilde{g}^{\gamma} \wedge d_2 = h^{\delta} \wedge d_1 = y_R^{\delta} g\gamma\}(m)$; $V_2 := SPK_{14}\{(\beta) : \tilde{z}\tilde{g} = \tilde{g}^{\beta'}\}(V_1)$; $V_3 := SPK_{12}\{(\alpha) : d = \tilde{g}^{\alpha'}\}(V_2)$*; wherein V_2, and V_3 are known as additional signatures).*

Camenisch does not explicitly disclose a fifth step of encrypting, at the first calculation means of the trusted authority, the common private key using each of the symmetrical secret keys to obtain as many encrypted forms of the common private key as there are non-revoked members; a seventh step of encrypting, at the first calculation means of the trusted authority, the up-to-date common private key using each of the symmetrical secret keys to obtain as many encrypted forms of the up-to-date common private key as there are non-revoked members; and an eighth step of updating the common private key stored in the storage means of the signing member only if one encrypted value of the up-to-date common private key may be decrypted using the symmetrical secret key stored in the storage means of the signing member.

However, in an analogous art, Inada discloses a method for group unit encryption/decryption, wherein:

a fifth step of encrypting, at the first calculation means of the trusted authority, the common private key using each of the symmetrical secret keys to obtain as many encrypted forms of the common private key as there are non-revoked members *(Inada: col. 19, lines 10-13; common key C_G is encrypted using P_{Mi} key)*;

a seventh step of encrypting, at the first calculation means of the trusted authority, the up-to-date common private key using each of the symmetrical secret keys to obtain as many encrypted forms of the up-to-date common private key as there are non-revoked members *(Inada: col. 19, lines 10-13; common key C_G is encrypted using P_{Mi} key)*; and

an eighth step of updating the common private key stored in the storage means of the signing member only if one encrypted value of the up-to-date common private key may be decrypted using the symmetrical secret key stored in the storage means of the signing member *(Inada: col. 22, lines55-60; the extracted $P_{Mi}(C_G)$ is decrypted by use of the individual key to acquire the common key C_G)*;

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Inada with the method and system of Camenisch to include steps of a fifth step of encrypting, at the first calculation means of the trusted authority, the common private key using each of the symmetrical secret keys to obtain as many encrypted forms of the common private key as there are non-revoked members; a seventh step of encrypting, at the first calculation means of the trusted authority, the up-to-date common private key using each of the symmetrical secret keys to obtain as many encrypted forms of the up-to-date common private key as there are non-revoked members; and an eighth step of updating the common private key stored in the storage means of the signing member only if one encrypted value of the up-to-date common private key may be decrypted using the symmetrical secret key stored in the storage means of the signing member to allow an arbitrary member in a group to decrypt

and write a signature by use of a group key which is allowed to be used by only the group member *(Inada: col. 1, lines 9-12)*.

Camenisch and Inada disclose all limitations as recited above but do not explicitly disclose on each revocation of a member from the group, the method further comprising: a sixth step of modifying, at the first calculation means of the trusted authority, the pair of asymmetric keys common to the group to create an up-to-date common public key and an up-to-date common private key;

However, in an analogous art, Kim discloses a method for efficient and secure member deletion in group signature schemes, wherein on each revocation of a member from the group, the method further comprising: a sixth step of modifying, at the first calculation means of the trusted authority, the pair of asymmetric keys common to the group to create an up-to-date common public key and an up-to-date common private key *(Kim: page 157; section 1.3; steps 1-3)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Kim with the method and system Camenisch and Inada wherein on each revocation of a member from the group, the method further comprising: a sixth step of modifying, at the first calculation means of the trusted authority, the pair of asymmetric keys common to the group to create an up-to-date common public key and an up-to-date common private key to allow member deletion and sign-tracing generated by a specific member *(Kim: page 151, lines 15-16)*.

- **Regarding claim 10**, Camenisch discloses a cryptographic system for anonymously signing a digital message, the system comprising:

first calculation means for calculating at least one of a pair of asymmetric keys common to members of a group of plural members and a group public key associated with the group *(Camenisch: page 100, section 5.4.1, lines 19-21; page 105, section 5.5.1, lines 16-17; RSA public key (n,e), the primes p and q are her secret key)* and said group public key (32) associated with the group *(page 101, lines 1-3; page 105, section 5.5.1, lines 29-30; group public key Y)*, for calculating said group private key for each member during interaction with a calculation means of the each member, each said group private key for each member being associated with said group public key and being different for each member of the group *(Camenisch: pages 101-102, section 54.2; pages 106-107, section 5.5.2: Generating Membership Keys and Certificate; Arto joins the group, obtains membership certificate, stores x, y, and v securely)*, for creating as many symmetrical secret keys as there are members of the group *(Camenisch: page 74, lines 13-15; a secret key x_i to each group member P_i)*, and means for storing said common private key, said group private key of the each member, and said symmetrical secret key assigned to the each member *(Camenisch: pages 101-102, section 54.2; pages 106-107, section 5.5.2: Generating Membership Keys and Certificate; Arto joins the group, obtains membership certificate, stores x, y, and v securely)*; and calculation means for calculating an anonymous signature for a message using said group private key of the each member and for calculating an additional signature for a combination comprising the message and the anonymous signature using said common private key *(Camenisch: Camenisch: pages 102-*

103 and 107-108; sections 5.4.3, 5.4.4, 5.5.3, and 5.5.4; signing messages and opening signature; $V_1 := SPK_{14}\{(\beta) : d\widetilde{g} = \widetilde{g}^{\beta r}\}(m)$ and $V_2 := SPK_{12}\{(\alpha) : d = \widetilde{g}^{\alpha r}\}(V_1)$; *also* $V_1 := SPK_7\{(\gamma, \delta) : \widetilde{z} = \widetilde{g}^{\gamma} \wedge d_2 = h^{\delta} \wedge d_1 = y_R^{\delta} g\gamma\}(m)$; $V_2 := SPK_{14}\{(\beta) : \widetilde{z}\widetilde{g} = \widetilde{g}^{\beta r}\}(V_1)$; $V_3 := SPK_{12}\{(\alpha) : d = \widetilde{g}^{\alpha r}\}(V_2)$*; wherein V_2, and V_3 are known as additional signatures).*

Camenisch does not explicitly disclose encrypting a common private key of said asymmetrical keys common to said members of the group using each of said symmetrical secret keys to obtain as many encrypted forms of said common private key as there are non-revoked members; and a smart card associated with each member in the group.

However, in an analogous art, Inada discloses a method for group unit encryption/decryption, wherein encrypting a common private key of said asymmetrical keys common to said members of the group using each of said symmetrical secret keys to obtain as many encrypted forms of said common private key as there are non-revoked members *(Inada: col. 19, lines 10-13; common key C_G is encrypted using P_{Mi} key; col. 22, lines55-60; the extracted $P_{Mi}(C_G)$ is decrypted by use of the individual key to acquire the common key C_G)*; and a smart card associated with each member in the group *(Inada: col. 1, lines 52-55 and 65-67)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Inada with the method and system of Camenisch to include steps of encrypting a common private key of said asymmetrical keys common to said members of the group using each of said symmetrical secret keys to obtain as many encrypted forms of said common private key as there are

non-revoked members; and a smart card associated with each member in the group to allow an arbitrary member in a group to decrypt and write a signature by use of a group key which is allowed to be used by only the group member *(Inada: col. 1, lines 9-12)*.

Camenisch and Inada disclose all limitations as recited above, but do not explicitly disclose means for updating said common private key stored in the storage means of the each member to update said common private key only if one encrypted value of said common private key calculated by said first calculation means may be decrypted using said symmetrical secret key in said storage means of the each member;

However, in an analogous art, Kim discloses a method for efficient and secure member deletion in group signature schemes, wherein means for updating said common private key stored in the storage means of the each member to update said common private key only if one encrypted value of said common private key calculated by said first calculation means may be decrypted using said symmetrical secret key in said storage means of the each member *(Kim: page 157; section 1.3; steps 1-3)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Kim with the method and system of Camenisch and Inada wherein means for updating said common private key stored in the storage means of the each member to update said common private key only if one encrypted value of said common private key calculated by said first calculation means may be decrypted using said symmetrical secret key in said storage means of the each member to allow member deletion and sign-tracing generated by a specific member *(Kim: page 151, lines 15-16)*.

- **Regarding claim 11**, claim 11 is similar in scope to claim 1, and is therefore rejected under similar rationale.

Allowable Subject Matter

- **Claims 2, 3, and 5 are objected to** as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

- **Claim 4 is objected to** as being dependent upon a rejected base claim. Claim 4 is dependent on claim 3, and would be allowable if claim 3 is rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

12. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Luu Pham whose telephone number is 571-270-5002. The examiner can normally be reached on Monday through Friday, 7:30 AM - 5:00 PM (EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Luu Pham/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437